



# Department of Homeland Security Daily Open Source Infrastructure Report for 05 January 2007

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The Washington Times reports federal officials are recommending new security measures to protect the nation's half-dozen liquefied natural gas facilities from a terrorist attack, after a break-in at a Massachusetts operation last summer went undetected for nearly a week. (See item [3](#))
- The Department of Homeland Security on Wednesday, January 3, announced the issuance of the final rule for the Transportation Worker Identification Credential program, which enhances port security by checking the backgrounds of workers before they are granted unescorted access to secure areas of vessels and maritime facilities. (See item [14](#))
- The Associated Press reports Rhode Island officials canceled school Thursday, January 4, for more than 20,000 students while health experts search for any connection between a suspected case of meningitis and a second-grader's encephalitis death two weeks ago. (See item [22](#))

### DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *January 03, CNET* — Wal-Mart readies large-scale move into solar power. Wal-Mart is looking to embark on what could be a massive solar power project — part of a long-term plan

to convert to renewable energy sources. Although Wal-Mart's bid may not result in any investment, the move is significant as an indicator of growing corporate interest in sustainable practices and technologies. If completed, it could amount to a significantly large installation — on the order of 100 megawatts of power over the next five years. "To put that into perspective, the solar system currently being installed at Google headquarters in California — the largest single corporate solar installation in history — is 1.6 MW, about 1/60th the size," wrote Joel Makower, a clean-technology consultant. Makower said the Wal-Mart proposal called for a system that could be replicated across its stores in five states and make use of available roofing space. Wal-Mart has set up experimental stores in McKinney, TX, and Aurora, CO, which are already using renewable power sources. Other large companies investing in renewable technologies on a large scale are Google and Microsoft, which has equipped its headquarters with more than 2,000 solar panels capable of generating 480 kilowatts at peak capacity.

Source: [http://news.com.com/Wal-Mart+readies+large-scale+move+into+solar+power/2100-11395\\_3-6146851.html](http://news.com.com/Wal-Mart+readies+large-scale+move+into+solar+power/2100-11395_3-6146851.html)

2. *January 03, Electric Light & Power* — **Con Edison announces new vegetation management program.** Consolidated Edison Co. (Con Edison) is initiating a three-year, enhanced tree-trimming program in hopes of preventing storm-related power outages throughout Westchester County, NY. The company estimates that the new program, starting this month, could result in a 20 percent reduction in the number of outages experienced during major storms. The effort will also help minimize public safety hazards created by windblown branches and broken limbs that bring down live power lines. "More than 50 percent of the outages experienced by customers during major storms in Westchester have been caused by tree-related damage," said William J. McGrath, Con Edison's VP of electric operations for Bronx/Westchester. The new initiative follows a series of outages triggered by overgrown trees in Westchester, particularly in September when tropical storm Ernesto downed trees, tree limbs and branches that extended onto power lines, causing outages to 76,000 customers. McGrath said, "...it's best to proactively trim to minimize the amount of emergency work that's needed later. Often these limbs pose risks to electric reliability and public safety, even during mild weather." Con Edison expects to trim approximately 85,000 trees annually in Westchester in a three-year cycle.

Source: [http://uaelp.pennnet.com/display\\_article/281232/22/ARTCL/non e/none/Con-Edison-announces-new-vegetation-management-program/](http://uaelp.pennnet.com/display_article/281232/22/ARTCL/non e/none/Con-Edison-announces-new-vegetation-management-program/)

3. *January 03, Washington Times* — **Security found lax at LNG sites.** Federal officials are recommending new security measures to protect the nation's half-dozen liquefied natural gas (LNG) facilities from a terrorist attack after a break-in at a Massachusetts operation last summer went undetected for nearly a week. In addition to regulations requiring security systems to deter intruders, the Transportation Department says the operation must be tested to "verify that alarms work and that monitoring devices function as intended," and that surprise testing should be conducted, according to an advisory released Friday, December 29. Personnel should be trained on security procedures, which should be updated and incorporated with the most relevant threat information, said the findings from the Pipeline and Hazardous Materials Safety Administration. There have been no major accidents or incidents involving the transport of liquefied natural gas, which has been delivered from overseas ports in Algeria, Libya, Egypt, Qatar, United Arab Emirates, Trinidad and Malaysia for 45 years. Since the September 11 terrorist attacks, the departments of Transportation and Homeland Security have joint

responsibility for LNG terminals, which some critics say pose security threats to nearby communities.

Source: <http://washingtontimes.com/national/20070102-111004-4755r.htm>

4. *January 03, Springfield News-Leader (MO)* — **Potential disaster at Missouri gasoline storage facility.** Workers using cutting torches inside an empty 1.5-million-gallon gasoline storage tank accidentally ignited a small pocket of undetected fuel Wednesday, January 3. All three workers escaped from the Magellan Pipeline Co. storage tank near Republic, MO. Republic Fire Chief Duane Compton said “They’ve got about 12 million gallons of gasoline and diesel stored out there.” The workers’ cutting torches ignited a small pocket of unleaded gasoline, which in turn ignited a secondary fire in the rubber sealing ring around the edge of the internal floating roof. When the tank is being used, the internal floating roof sits directly on the fuel and helps keep explosive fumes from building up inside. Republic firefighters quickly cooled down the internal roof with water and extinguished the fire burning in the rubber seal. Source: <http://www.news-leader.com/apps/pbcs.dll/article?AID=/20070103/BREAKING01/70103028>

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

5. *January 04, Associated Press* — **Plant employee dies after inhaling hydrogen fluoride.** A South Texas man has died after inhaling hydrogen fluoride gas while working in the chemical department of an Alcoa plant in Point Comfort, TX. Alcoa officials identified the man Wednesday, January 3, as John Dorton of Port Lavaca. Dorton came in contact with the gas Tuesday while working in the area of the plant that makes aluminum fluoride, which is used in the production of aluminum. The preliminary investigation indicates that the exposure happened Tuesday afternoon as Dorton worked near a valve. Dorton was pronounced dead seven hours later at Memorial Hermann Hospital in Houston, where he was taken by air ambulance after being treated at a Victoria hospital. Source: <http://thefacts.com/texasstory.lasso?ewcd=096052bc2229454a>

[[Return to top](#)]

## **Defense Industrial Base Sector**

6. *January 03, Reuters* — **Japan set to spend millions on missile defense.** Japan may be getting set to pour hundreds of millions of dollars into plugging missile defense gaps demonstrated by North Korea's July test firings, a Lockheed Martin executive said Wednesday, December 3. Also being discussed is removing "barriers" to coordination with the United States to thwart missiles that could be tipped with chemical, biological or nuclear warheads, said Ed Butt, head of a Lockheed missile defense division. "Over a period of five years, we're talking about a few hundred million dollars" in Japanese investments, potentially in command and control systems of its own, as well as in U.S. solutions, Butt said in a teleconference with reporters. Japan is working through issues tied to how far it may go in coordinating its missile defenses with the United States under its U.S.-imposed pacifist constitution.

Source: [http://money.cnn.com/2007/01/03/news/international/japan.reu.t/index.htm?source=yahoo\\_quote](http://money.cnn.com/2007/01/03/news/international/japan.reu.t/index.htm?source=yahoo_quote)

7. *January 03, Air Force* — **Air Force leaders develop strategic view on fuels.** Air Force leaders from major commands met recently to discuss the service's strategic viewpoint on fuel conservation. As the Department of Defense's greatest fuel consumer, the Air Force must examine every aspect of fuel consumption while maintaining its core competencies and power–projection capabilities, said Col. Anne Dunlap, Air Force Conduct Air, Space and Cyber Operations core team leader at the Pentagon. "All the major commands gathered to examine multiple aspects of fuel–savings potential, such as simulation, aircraft training, logistics efficiencies, scheduling, acquisition and technology developments and flying operations," she said. The group used Air Force Smart Operations for the 21st century techniques during the event, looking at the Air Force vision for fuels efficiency, goals for air operations and barriers to success to build a game plan for how to best conserve fuel efficiently and effectively.
- Source: <http://www.af.mil/news/story.asp?id=123036579>

[[Return to top](#)]

## **Banking and Finance Sector**

8. *January 04, VNUNet* — **U.S. tax payers targeted in phishing scam.** Americans now have another reason to dread the tax season, following a warning from the U.S. Computer Emergency Response Team (US–CERT) of phishing attacks targeting the Internal Revenue Service (IRS). The IRS has become the target of new phishing scams that claim to offer tax refunds. Recipients are asked to enter personal information into an online form which can then be used by identity thieves. Government sites have been largely ignored by phishers, who favor e–commerce hubs such as eBay and PayPal and large regional banks.
- Source: <http://www.vnunet.com/vnunet/news/2171829/phishers-look-happy-tax-season>
9. *January 04, Associated Press* — **Treasury steps up pressure on Syria.** The Bush administration, intensifying pressure on Damascus, moved Thursday, January 4, to financially clamp down on three Syrian institutions suspected of helping spread weapons of mass destruction. The Treasury Department's action means that any bank accounts or financial assets belonging to the three entities found in the United States would be frozen. Americans also are prohibited from doing business with them. The three entities targeted are the Higher Institute of Applied Science and Technology, the Electronics Institute, and the National Standards and Calibration Laboratory. "Syria is using official government organizations to develop nonconventional weapons and the missiles to deliver them," Stuart Levey, Treasury's under secretary for terrorism and financial intelligence, said in explaining the United States' action. The three entities acted against Thursday are "subordinates" of the Scientific Studies and Research Center, the Syrian government agency responsible for developing and producing non–conventional weapons and the missiles to deliver them, the department said.
- Source: [http://biz.yahoo.com/ap/070104/terror\\_financing.html?.v=1](http://biz.yahoo.com/ap/070104/terror_financing.html?.v=1)
10. *January 03, Bankrate* — **States pass laws dealing with child identity theft.** Several states have passed laws over the past three years designed to safeguard children from financial

scammers. These include California's Chapter 387, which requires a county welfare department to request a consumer disclosure, on behalf of a youth in a foster care placement in the county when the youth reaches his or her 16th birthday in order to ascertain whether the youth has been the victim of identity theft; Florida's Chapter 32, which provides an exemption from public record requirements for the names, home addresses, telephone numbers, Social Security numbers and photographs of children who participate in government-sponsored recreation programs or camps; Nevada's Chapter 90, which protects the confidentiality of certain personal identifying information of parents and children involved in paternity cases by removing the requirement that the court include such information in its orders that are available to the public; Virginia's Chapter 500, which requires that the record of any divorce suit not contain the Social Security number of any party or of any minor child, or any financial information; and Wyoming's Chapter 155, which makes financial information provided by parties for child support confidential, removes parties' Social Security numbers from divorce decrees.

Source: <http://biz.yahoo.com/brn/070103/20493.html?v=1>

[\[Return to top\]](#)

## **Transportation and Border Security Sector**

11. *January 04, Miami Herald* — **Port for calls: Cruise ships go cellular.** Miami-based Carnival Cruise Lines and top competitor Royal Caribbean Cruises International last month finished outfitting their fleets so passengers can use their own cell phones virtually anywhere onboard. They are among a host of cruise lines adding cell phone service, the latest technology offered at sea to connect passengers to land. "You can send text messages and use your BlackBerry just like on land," says Carnival spokesperson Vance Gulliksen. The dilemma of cell service has provoked much hand wringing over how to balance the desire to get away with the need to stay connected, say cruise lines. Passengers have gravitated to cable TV, Internet cafes, and, most recently, WiFi Internet service, which was completed on Royal Caribbean ships last January. Cell phone service was "the next logical step," says Chip Norcross, manager of onboard revenue for Royal Caribbean. Norwegian Cruise Line became first to go fleetwide with the service in July. Celebrity Cruises is rolling it out now, with two of its nine ships complete. Source: <http://www.miami.com/mld/miamiherald/business/16378569.htm>

12. *January 04, Seattle Times* — **Ferries study warns: no money for projects.** Washington State Ferries are in such tough financial shape, there's no way to pay for \$410 million in capital projects such as new boats and ferry terminals. Further, because of high labor and fuel costs, ferry management "has little opportunity to control operating costs effectively. The gap in capital funding is likely to be the largest financial problems facing Washington State Ferries." These were among the findings in a draft of a new, 67-page ferries-financing study given Wednesday, January 3, to the state Legislature's Joint Transportation Committee. The study, ordered by the Legislature, was conducted by a team of consultants, including the Cedar Rivers Group. Among other suggestions was one certain to be controversial: raising peak-hour ferry fares. The study was ordered to try to figure out how to finance the state's ferry system after it took a huge hit in 1999 with the passage of an initiative that slashed the state's motor-vehicle excise tax, which helped finance ferry operations.

Source: [http://seattletimes.nwsources.com/html/localnews/2003508574\\_ferry04m.html](http://seattletimes.nwsources.com/html/localnews/2003508574_ferry04m.html)



13. *January 04, Associated Press* — **FAA: Atlanta airport is nation's busiest.** For the second year in a row, Hartsfield–Jackson Atlanta International Airport has retained its title as the nation's busiest in terms of flights, according to government data released Thursday, January 4. Chicago O'Hare International Airport, was listed second busiest airport. Atlanta and Chicago have run neck-and-neck in recent years to claim the title of the nation's — and therefore, the world's — busiest airport. Atlanta already claimed to be the world's busiest airport in terms of passengers. Flights include takeoffs and landings. The FAA does not maintain passenger statistics. Atlanta airport spokesperson Sterling Payne said opening a fifth runway in May benefited the airport and last year's expansion of international flights by Delta Air Lines Inc. — which has its primary hub in Atlanta — also was another factor that caused the Atlanta airport to remain the nation's busiest.

Source: [http://biz.yahoo.com/ap/070104/busy\\_airports.html?v=2](http://biz.yahoo.com/ap/070104/busy_airports.html?v=2)

14. *January 03, Transportation Security Administration* — **DHS issues credentialing rule to secure access to U.S. ports.** The Department of Homeland Security (DHS) on Wednesday, January 3, announced the issuance of the final rule for the Transportation Worker Identification Credential (TWIC) program, which enhances port security by checking the backgrounds of workers before they are granted unescorted access to secure areas of vessels and maritime facilities. The rule was posted publicly on Transportation Security Administration's (TSA) Website January 1, 2007, and has been delivered to the Federal Register for posting in the coming days. The rule lays out the enrollment process, disqualifying crimes, usage procedures, fees, and other requirements for workers, port owners, and operators. These guidelines allow the industry, government and public to prepare for the implementation of this important security program. The TSA and the U.S. Coast Guard held four public meetings around the nation and received more than 1,900 comments regarding the initial draft of this federal rule. Comments were filed by workers, port facility owners and operators, small businesses and others who would be affected by the new program. The rule is expected to impact more than 750,000 port employees, longshoremen, mariners, truckers and others who require unescorted access to secure areas of ports and vessels.

TWIC Implementation in the Maritime Sector final rule

[http://www.tsa.gov/assets/pdf/1652-AA41\\_twic\\_fr.pdf](http://www.tsa.gov/assets/pdf/1652-AA41_twic_fr.pdf)

U.S. Coast Guard's Homeport information: <http://homeport.uscg.mil/mycg/portal/ep/home.do>

TWIC program: [http://www.tsa.gov/what\\_we\\_do/layers/twic/index.shtm](http://www.tsa.gov/what_we_do/layers/twic/index.shtm) and's Homeport s

Source: [http://www.tsa.gov/press/releases/2007/press\\_release\\_01032007.shtm](http://www.tsa.gov/press/releases/2007/press_release_01032007.shtm)

[\[Return to top\]](#)

## **Postal and Shipping Sector**

15. *January 03, NBC4 (DC)* — **Suspicious letter sent to Reagan Building.** A Hazmat situation is over after officials investigated a suspicious letter that was sent to the Ronald Reagan Building in northwest Washington, DC. Hazmat crews went to the building at the corner of 14th and D streets because of the letter, which was sent by a prisoner to Immigration and Customs Enforcement. The letter had the word "anthrax" written on it, and it initially appeared to be from Brazil, authorities said. The letter had a suspicious substance in it, which was contained in a plastic bag, officials said. The substance turned out to be brewer's yeast. The package had been irradiated before it arrived at the Reagan Building, according to fire officials. The FBI is

investigating.

Source: <http://www.nbc4.com/news/10662671/detail.html>

[\[Return to top\]](#)

## **Agriculture Sector**

**16. *January 04, Mail Tribune (OR)* — Groups aim to shut down captive elk–ranching industry.**

Animal–rights and hunting groups again are taking a collective run at closing Oregon's captive elk–ranching industry over fears the exotic herds threaten wild elk populations. But this time, the so–called MAD–elk Coalition has found fresh wind in its sails thanks to the misfortunes of an Idaho elk rancher whose animals escaped last summer, threatening the health and gene pool of Yellowstone's elk. Backers say they don't want an Oregon ranch to repeat the escape of more than 100 exotic elk in Idaho, where the state's governor has ordered the wayward animals shot before they can interbreed with native elk. Now the coalition here has support from the Oregon Department of Fish and Wildlife in calling for the drafting of new rules that would increase fencing restrictions on the remaining 16 elk ranches in Oregon and ban any transfers of ranching licenses. That would mean current ranches would be further isolated from any contact with wild elk. Eventually, the practice of raising elk for meat and antler sales would eventually disappear when current ranchers die or fold their businesses.

Source: <http://www.mailtribune.com/archive/2007/0104/sport/stories/cervidpetition–freecol.htm>

**17. *January 04, Chronicle Herald (Canada)* — Anemia disease has devastated fish farms in**

**New Brunswick.** The Canadian government is studying a virus that can devastate salmon farms. Infectious salmon anemia forced New Brunswick salmon farmers to slaughter more than a million fish nearly a decade ago. It was discovered in farmed Nova Scotia salmon in 1999 but in much smaller numbers. "It has the potential to spread to other species and be a disease of national significance and have a big impact on trade," said Archie Stewart, acting director of the Canadian Food Inspection Agency's aquatic animal health division. The agency wants to determine whether the virus can be eradicated or managed, said the veterinarian. Canada is considering making infectious salmon anemia a reportable disease. That would mean veterinarians, fish farmers and laboratories must inform the feds of any suspected outbreak. The disease first appeared at fish farms in Norway almost two decades ago, then in New Brunswick and later Scotland. It has also been discovered in Maine.

Infectious salmon anemia information: <http://www.aphis.usda.gov/lpa/pubs/tnisa.html>

Source: <http://thechronicleherald.ca/NovaScotia/550550.html>

[\[Return to top\]](#)

## **Food Sector**

**18. *January 03, Food Safety and Inspection Service* — Cheese products recalled.**

Pap's Louisiana Cuisine, a Prairieville, LA, firm, is voluntarily recalling approximately 290 pounds of head cheese products that may be contaminated with *Listeria monocytogenes*, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Wednesday, January 3.

The head cheese products were distributed to retail establishments in Southeast Louisiana. The problem was discovered through the FSIS routine microbiological testing. FSIS has received no reports of illnesses associated with consumption of this product. Consumption of food contaminated with *Listeria monocytogenes* can cause listeriosis, an uncommon but potentially fatal disease.

Source: [http://www.fsis.usda.gov/News\\_&\\_Events/Recall\\_001\\_2007\\_Release/index.asp](http://www.fsis.usda.gov/News_&_Events/Recall_001_2007_Release/index.asp)

19. *January 03, Reuters* — **White House clears proposal for older Canada cattle.** The White House has approved a draft U.S. regulation that would allow imports of older Canadian cattle and beef into the country, now blocked out of concerns over mad cow disease. With the time needed for the U.S. Department of Agriculture to review public comments and suggestions for changes, it could be "sometime in the summer" before U.S. import rules were revised, said an official of the National Cattlemen's Beef Association. At present, cattle less than 30 months of age can be shipped for slaughter at U.S. packing plants and Canadian packers can send beef from young cattle to U.S. buyers.

Source: [http://ca.today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2007-01-03T235409Z\\_01\\_N03402408\\_RTRIDST\\_0\\_CA\\_NADA-MADCOW-USA-USDA-COL.XML&archived=False](http://ca.today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2007-01-03T235409Z_01_N03402408_RTRIDST_0_CA_NADA-MADCOW-USA-USDA-COL.XML&archived=False)

20. *January 03, Farmer's Weekly (United Kingdom)* — **Human campylobacter infection rates overtake salmonella in European Union.** An European Union (EU) report announced last month that more EU citizens were infected with campylobacter than salmonella in 2005. The European Food Safety Authority (EFSA) stated that campylobacter rates increased by 7.8 percent over one year — amounting to 197,363 cases in 2005. In contrast, salmonella infection rates decreased by 9.5 percent in 2005 with 176,395 reported cases. The primary source of infection for human cases of campylobacter was fresh poultry meat, with 66 percent of samples testing positive. And that 80 percent of tested campylobacter bacteria was resistant to human antibiotics.

Source: <http://www.fwi.co.uk/Articles/2007/01/03/100475/human-campylobacter-infection-rates-overtake-salmonella-in.html>

21. *January 02, Consumer Reports* — **Bacteria found on poultry.** Consumer Report's (CR) analysis of fresh, whole broilers bought nationwide revealed that 83 percent harbored campylobacter or salmonella, the leading bacterial causes of foodborne disease. That's an increase from 2003, when CR reported finding that 49 percent tested positive for one or both pathogens. Leading chicken producers have stabilized the incidence of salmonella, but spiral-shaped campylobacter has is on more chickens than ever. CR tested 525 fresh, whole broilers bought at supermarkets, mass merchandisers, gourmet shops, and -natural-food stores in 23 states. Represented in the tests were four leading brands and 10 organic and 12 nonorganic no-antibiotics brands, including three that are "air chilled" in a newer slaughterhouse process designed to reduce contamination. Campylobacter was present in 81 percent of the chickens, salmonella in 15 percent; both bacteria in 13 percent. Only 17 percent had neither pathogen. That's the lowest percentage of clean birds in all four CR tests since 1998. Among all brands, 84 percent of the salmonella and 67 percent of the campylobacter organisms we analyzed showed resistance to one or more antibiotics.

Source: [http://www.consumerreports.org/cro/food/chicken-safety-1-07/overview/0107\\_chick\\_ov.htm](http://www.consumerreports.org/cro/food/chicken-safety-1-07/overview/0107_chick_ov.htm)



[\[Return to top\]](#)

## **Water Sector**

Nothing to report.

[\[Return to top\]](#)

## **Public Health Sector**

### **22. *January 04, Associated Press* — More than 20,000 students kept home after illness report.**

Rhode Island officials canceled school Thursday, January 4, for more than 20,000 students while health experts search for any connection between a suspected case of meningitis and a second-grader's encephalitis death two weeks ago. Rhode Island health officials are investigating a link between the illness of a student at Hopkins Hill School in Coventry reported late Wednesday and mycoplasma, an infection blamed for encephalitis that killed a Warwick student and sickened two other children. Meningitis is an inflammation of membranes protecting the brain and spinal cord that requires hospitalization in severe cases. Encephalitis also involves brain inflammation caused by a virus. Officials said more epidemiologists from the U.S. Centers for Disease Control and Prevention are headed to the state to assist the half-dozen scientists already in Rhode Island. Health investigators will spend the next few days talking to school nurses and looking for possible additional cases in hospitals. A second-grade student at Warwick's Greenwood Elementary School, died last month after mycoplasma progressed to encephalitis. One of his classmates also suffered from a mild case of encephalitis but has recovered. A third student at a West Warwick middle school was also infected but has since recovered.

Source: [http://www.boston.com/news/local/rhode\\_island/articles/2007/01/04/ri\\_health\\_officials\\_close\\_schools\\_in\\_three\\_towns/](http://www.boston.com/news/local/rhode_island/articles/2007/01/04/ri_health_officials_close_schools_in_three_towns/)

### **23. *January 03, Mercury News (CA)* — Suspected virus closes San Quentin Prison to visitors, new inmates.**

San Quentin State Prison has been closed to new inmates, visitors and volunteers because of an outbreak of an illness suspected to be norovirus, the California Department of Corrections and Rehabilitation reported Wednesday, January 3. The illness that causes diarrhea, vomiting, abdominal cramps, headache and fever was first detected December 28 and has affected at least 489 inmates and six staff members. The prison has been closed to all intakes and transfers and all inmate movement has been temporarily restricted, state officials said. Inmates with symptoms are being confined to their quarters and are being fed in their cells. Inmates' medical appointments for non-urgent care in community facilities have been canceled and inmates will not be transferred for court appearances until they are medically screened. Common areas of the prison are being cleaned and disinfected. San Quentin medical officials have informed county and state officials of the outbreak and have sent cultures to independent labs to determine the cause of the illness and monitor its progression. Seventeen Northern California counties send between 50 and 125 inmates to San Quentin State Prison each week.

Source: [http://www.mercurynews.com/mld/mercurynews/news/local/163773\\_43.htm](http://www.mercurynews.com/mld/mercurynews/news/local/163773_43.htm)

### **24. *January 03, University of Georgia* — Study underscores importance of rapid response in**

**curtailing disease outbreaks.** A University of Georgia (UGA) study suggests that rapid detection combined with aggressive education can dramatically curtail outbreaks of emerging infectious disease. John Drake, assistant professor in the UGA Institute of Ecology, has created a mathematical model that takes into account how factors such as the speed at which information is gathered about a disease and how quickly that information is disseminated to the public affect the final size of an outbreak. One finds that in the 2003 Severe Acute Respiratory Syndrome (SARS) outbreak in Singapore, doubling the rate at which infected people removed themselves from the larger population by quarantining themselves or seeking treatment would have cut the total number of infected people from 238 to 116. If infected individuals had removed themselves at half the actual rate, the number of cases would have ballooned to nearly 800. Drake said that with modifications to account for differences in factors such as transmission rate, the model can be applied to other emerging infectious diseases such as avian influenza. Drake's model has the potential to estimate outbreak size based on: the transmission rate, infectious period, the removal rate and the rate at which the public health response begins to produce diminishing returns.

Source: [http://www.uga.edu/news/artman/publish/070103Rapid\\_reponse\\_curtailing\\_disease\\_outbreak.shtml](http://www.uga.edu/news/artman/publish/070103Rapid_reponse_curtailing_disease_outbreak.shtml)

- 25. *January 01, National Institutes of Health* — New details on how the immune system recognizes influenza.** Drawing upon a massive database established with funds from the National Institute of Allergy and Infectious Diseases (NIAID), one of the National Institutes of Health (NIH), scientists have completed the most comprehensive analysis to date of published influenza A virus epitopes — the critical sites on the virus that are recognized by the immune system. The study should help scientists who are designing new vaccines, diagnostics and immune-based therapies against seasonal and pandemic influenza because it reveals in molecular detail exactly where the immune system focuses on the viruses. Although the complete molecular structures of essentially all major strains of influenza viruses are known, immune responses concentrate on limited regions of certain parts of the virus, and these regions must be identified as immune epitopes by research studies. Researchers found that while there were hundreds of shared epitopes among different virus strains only one has been published that appears ideal for multi-strain vaccines. Information on shared protective epitopes is important for developing influenza vaccines that can provide broad protection against multiple strains of the virus. The researchers have also built numerous tools for analyzing and visualizing the data and for predicting immunity against different pathogens.

Tools: <http://immuneepitope.org>

Source: <http://www.nih.gov/news/pr/jan2007/niaid-01.htm>

[\[Return to top\]](#)

## **Government Sector**

- 26. *January 04, Detroit Free Press* — Michigan teen charged with school threats.** A 17-year-old from Rochester Hills, MI, has been charged with threatening to shoot six students at his high school last month. Brandon Worden was arraigned Tuesday in Rochester Hills on charges of making a false report of terrorism and using a computer to commit a crime. On December 4, Worden sent an instant message to his 15-year-old ex-girlfriend saying that he was going to come to ACE (Alternative Center for Education) High School with a gun to shoot

six people, according to the Oakland County Sheriff's Office. The next day the school was temporarily put on lockdown and Worden was suspended. Later that week, he was expelled. Then, on December 24, Worden was arrested after he and a 16-year-old broke into Reuther Middle School in Rochester Hills. Worden was charged with breaking and entering and illegal entry. He was given a \$7,500 personal bond and ordered to wear an electronic monitoring tether.

Source: [http://www.freep.com/apps/pbcs.dll/article?AID=/20070104/NEW\\_S99/70104027](http://www.freep.com/apps/pbcs.dll/article?AID=/20070104/NEW_S99/70104027)

27. *January 03, ABC (CA)* — **Teens caught throwing homemade explosives at California federal building.** Two teenagers were taken into custody this morning, accused of throwing homemade bombs at Fresno's old Federal building. Police say they saw a 14-year-old and a 16-year-old boy tossing a plastic soda bottle over the fence of the old federal building in downtown Fresno, CA. Investigators say the kids put fireworks inside the bottle and watched as it exploded. Police say they were about to light up another one when they were caught in the act. The kids were cited with misdemeanors and released to their parents.

Source: <http://abclocal.go.com/kfsn/story?section=local&id=4902626>

[[Return to top](#)]

## **Emergency Services Sector**

28. *January 03, United Press International* — **Vibrating vest "talks" to wearer.** A vibrating vest that could warn soldiers or firefighters of danger when ordinary radios can't be used is being tested by U.S. researchers. The vest "writes" messages on the wearer's back, similar to Braille, by using 16 vibrating motors. Messages are transmitted wirelessly to the vest's receiver from a computer. Developers said the back was chosen because it is a relatively large area and unlikely to be injured. The U.S. Army, which is partially funding the project, is interested "in a way to communicate simple commands in situations when the hands are doing other things, or radios can't be used," said Lynette Jones, the Massachusetts Institute of Technology engineer leading the project. She said 15 symbols have been created already; eight of which are used by the military.

Source: <http://www.sciencedaily.com/upi/index.php?feed=Science&article=UPI-1-20070103-20174100-bc-us-vibratingvest.xml>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

29. *January 04, InfoWorld* — **Cisco buys e-mail security firm for \$830 million.** Cisco Systems Inc. said on Thursday, January 4, that it was buying IronPort Systems Inc. of San Bruno, CA, for \$830 million in cash and stock. The deal for privately held IronPort, which makes e-mail, Web, and security management appliances, will add expertise in spam and messaging security to Cisco's security portfolio. Cisco plans to use that technology as part of its Self-Defending Network framework, the company said in a statement. The deal is expected to close in the third quarter of Cisco's fiscal year 2007, which ends in April.

Source: [http://www.infoworld.com/article/07/01/04/HNciscoironport\\_1.html](http://www.infoworld.com/article/07/01/04/HNciscoironport_1.html)

30. *January 04, New York Times* — **U.S. bars lab from testing electronic voting.** A laboratory that has tested most of the nation's electronic voting systems has been temporarily barred from approving new machines after federal officials found that it was not following its quality-control procedures and could not document that it was conducting all the required tests. The company, Ciber Inc. of Greenwood Village, CO, has also come under fire from analysts hired by New York State over its plans to test new voting machines for the state. New York could eventually spend \$200 million to replace its aging lever devices. Experts on voting systems say the Ciber problems underscore longstanding worries about lax inspections in the secretive world of voting-machine testing. The action by the federal Election Assistance Commission seems certain to fan growing concerns about the reliability and security of the devices. Ciber, the largest tester of the nation's voting machine software, says it is fixing its problems and expects to gain certification soon. Experts say the deficiencies of the laboratory suggest that crucial features like the vote-counting software and security against hacking may not have been thoroughly tested on many machines now in use.  
Source: <http://www.nytimes.com/2007/01/04/washington/04voting.html?ref=us>

31. *January 04, Reuters* — **Three cell phone makers are sued over Bluetooth technology.** A United States research institute has sued three cell phone makers, accusing them of violating a patent for Bluetooth technology. The Washington Research Foundation, which markets technology from universities and other nonprofit research institutions in Washington State, is seeking damages from Nokia, Samsung Electronics and Panasonic, owned by Matsushita, contending that the three companies were using a radio frequency receiver technology patented by a University of Washington scientist in 1999. The suit was filed December 21 in Federal District Court in Seattle. The claim appears to restrict itself to Bluetooth devices sold or used in the United States, which means any ruling will affect around 15 to 20 percent of total global sales of Bluetooth mobile phones and headsets in the near term, according to Neil Mawston, an analyst at the market research group Strategy Analytics. But Ben Wood, a consultant at CCS Insight, said the implications for the standard could be more serious if the foundation's claim was successful. "A standard which everyone assumes to be royalty-free is now at risk of becoming a chargeable element inside mobile phones and other devices," he said.  
Source: <http://www.nytimes.com/2007/01/04/technology/04bluetooth.html>

32. *January 04, Security Focus* — **IE users at risk for 284 days in 2006.** Exploits and unpatched critical vulnerabilities put the users of Internet Explorer (IE) at risk 77 percent of the time last year, according to the latest number crunching by Brian Krebs of the Washington Post's Security Fix blog. Based on data published by Microsoft and interviews with researchers, Krebs found that critical security issues remained unpatched in IE for 284 days during 2006. The Mozilla Foundation's Firefox browser only suffered a single period of vulnerability lasting nine days, according to the analysis.  
Source: <http://www.securityfocus.com/brief/400>

33. *January 03, CNET News* — **Adobe flaw could spawn Web attacks.** A security weakness in the ubiquitous Acrobat Reader software could be a boon for cybercrooks, security experts warned Wednesday, January 3. An error in the Web browser plug-in of Adobe Systems' tool lets cybercrooks co-opt the address of any Website that hosts an Adobe PDF file for use in attacks, Symantec and VeriSign iDefense said. An attacker could construct seemingly trusted

links and add malicious JavaScript code that will run once the link is clicked, they said. "This vulnerability makes it possible for cross-site-scripting (XSS) attacks to occur, to steal cookies, session information, or possibly create a XSS worm," said Ken Dunham, director of the Rapid Response Team at VeriSign iDefense. The Adobe vulnerability could spark a rise XSS attacks, Symantec said. Such attacks in the past relied on flaws in Websites, but with the Adobe Reader bug there is now a widely used client-side application that allows cross-site-scripting attacks. Source: [http://news.com.com/Acrobat+flaw+could+spawn+Web+attacks/2100-1002\\_3-6147038.html](http://news.com.com/Acrobat+flaw+could+spawn+Web+attacks/2100-1002_3-6147038.html)

34. *January 02, New York Times* — **Rolling Wi-Fi hotspot to be offered in rental cars.** Try connecting to a high-speed wireless network from a car, and you are pretty much limited to one method: rigging your laptop computer with a special modem and subscribing to a costly, and sometimes temperamental, wireless service. But a start-up wireless technology company based in San Francisco is expected to announce this week that it has reached an agreement with a rental car company to provide a rolling Wi-Fi hotspot to customers by March. For \$10.95 a day, the rental car company will issue motorists a notebook-size portable device that plugs into a car's power supply and delivers a high-speed Internet connection. A mobile Wi-Fi hotspot that lets laptops and personal digital assistants link to the Internet without the benefit of wires represents an important step toward what technology experts call the "connected car." Users of these new Wi-Fi hotspots still must contend with technological limitations, like bandwidth restrictions and, for vehicles with too few auxiliary power outlets for all passengers who want to be online at the same time, battery consumption. Source: [http://www.nytimes.com/2007/01/02/technology/02avis.html?\\_r=1&adxnnl=1&oref=slogin&adxnnlx=1167919850-OdcMiLY20XTeAqD5K5 VT/w](http://www.nytimes.com/2007/01/02/technology/02avis.html?_r=1&adxnnl=1&oref=slogin&adxnnlx=1167919850-OdcMiLY20XTeAqD5K5 VT/w)

### Internet Alert Dashboard

Current Port Attacks	
<b>Top 10 Target Ports</b>	6881 (bittorrent), 1026 (win-rpc), 2967 (ssc-agent), 25 (smtp), 4672 (eMule), 80 (www), 6346 (gnutella-svc), 139 (netbios-ssn), 4662 (eDonkey2000), 445 (microsoft-ds)
Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center	
To report cyber infrastructure incidents or to request information, please contact US-CERT at <a href="mailto:soc@us-cert.gov">soc@us-cert.gov</a> or visit their Website: <a href="http://www.us-cert.gov">www.us-cert.gov</a> .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <a href="https://www.it-isac.org/">https://www.it-isac.org/</a> .	

[\[Return to top\]](#)

## Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

## General Sector

Nothing to report.



## **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS Daily Report Team at (703) 983–3644.
Subscription and Distribution Information:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.